Las Capacidades de Vigilancia de la NSA Según los Documentos de Snowden

Bonifaz Rafael
rafael@bonifaz.ec

Resumen.- En el año 2013, Edward Snowden filtró miles de documentos a los periodistas Glenn Greenwald y Laura Poitras. Parte de los mismos fueron publicados en investigaciones periodísticas en medios de comunicación alrededor del mundo. Este trabajo analiza los reportajes periodísticos y documentos publicados para entender como la NSA recolecta y analiza comunicaciones. Adicionalmente se muestran algunas de las operaciones de espionaje reveladas por los documentos.

Este trabajo publicó originalmente en el "IX Congreso Iberoamericano de Seguridad Informática" (CIBSI), que se realizó del 1 al 3 de noviembre de 2017 en la Universidad de Buenos Aires - Argentina[1].

Palabras claves: NSA, Vigilancia, Privacidad, Snowden

I. INTRODUCCIÓN

La Agencia Nacional de Seguridad de los Estados Unidos (NSA por sus siglas en inglés) se encarga de recolectar comunicaciones a nivel global para analizarlas y generar inteligencia. En el año 2013 Edward Snowden, contratista de la agencia, filtró miles de documentos secretos a los periodistas Glenn Greenwald y Laura Poitras. Estos documentos han evidenciado la capacidad de vigilancia de la NSA y el trabajo coordinado que realiza con empresas tecnológicas vulnerando la privacidad de las comunicaciones digitales a nivel mundial.

Desde junio de 2013 a la fecha se han publicado varios reportajes de prensa en diversos medios de comunicación al rededor del mundo. La Courage Foundation, organización que protege a denunciantes, administra el portal edwardsnowden.com donde, al momento de escribir este artículo, se han publicado 1530 documentos del archivo de Snowden. Cada uno de estos documentos está enlazado con los artículos de prensa que los referencia. De esta manera se podría saber si un documento se publicó en The Guardian, Washington Post, de The Intercept u otro.

Las fuentes utilizadas para las secciones dos, tres y cuatro de este trabajo son varios de los documentos que filtró Snowden, las publicaciones de prensa donde se hicieron públicos estos documentos, el libro "Snowden. Sin un Lugar Donde Esconderse" escrito por Glenn Greenwald y artículos de terceros que permiten contextualizar la información analizada.

Los artículos de prensa referenciados corresponden a medios de comunicación a los cuales Greenwald o Poitras dieron acceso a ciertos documentos. Específicamente se citan reportajes de The Guardian de Inglaterra, Der Spiegel de Alemania, L'Espresso de Italia, The New York Times de Estados Unidos, The Washinton Post de Estados Unidos, O Globo de Brasil y el medio digital The Intercept fundado por Glenn Greenwald.

1http://cibsi2017.org/

El portal Electrospaces.net ha profundizado el análisis de los documentos publicados con una visión crítica. Esto lo hace una fuente importante que facilita la comprensión de los programas revelados. Adicionalmente se hace referencia a noticias de prensa publicadas en la época cuando se hicieron públicos los documentos.

Si bien existe mucha información publicada sobre la filtración de Snowden estas son historias sueltas que muestran partes específicas del funcionamiento de esta agencia. Este trabajo organiza la información publicada para que de esta manera se pueda tener una visión sistémica del funcionamiento de la NSA. La metodología utilizada es de investigación bibliográfica y análisis exploratorio de la documentación publicada con el objetivo de conocer cómo recolecta información, la analiza y realiza operaciones de espionaje.

El tercer capítulo del libro "Snowden. Sin un Lugar Donde Esconderse" muestra las capacidades de la NSA según documentos publicados hasta 2014. A diferencia de ese capítulo, aquí se presenta la información organizada y todas las fuentes por donde se puede profundizar la investigación de cualquiera de los temas presentados. Este documento sirve como una primera lectura para profundizar la investigación sobre el funcionamiento de la NSA.

En primer lugar se analiza como la NSA recolecta miles de millones de comunicaciones a nivel global. Esto lo puede hacer gracias al trabajo coordinado con empresas norteamericanas de telecomunicaciones y servicios en Internet, la colaboración con agencias de otros países, a través de ataques informáticos, operaciones en misiones diplomáticas alrededor del mundo y a través de la interceptación de señales satelitales.

En segundo termino, se muestra como la información puede ser procesada en sistemas como XKEYSCORE que funciona de manera similar al buscador de Google pero sobre comunicaciones privadas. Para el año 2009 podía analizar contenido de comunicaciones hasta por tres días y metadatos hasta treinta días.

En tercer lugar, se verán algunas operaciones que ha realizado la NSA a presidentes, políticos, países y organizaciones internacionales con el fin de obtener beneficios para el gobierno de Estados Unidos y sus aliados.

Por último se realiza una breve descripción de como podrían operar agencias de inteligencia de otros países gracias al software y hardware de vigilancia disponible para gobiernos. Las fuentes son las revelaciones Spy Files publicadas en Wikileaks entre los 2011 a 2014, así como también noticias que hacen referencia a estas filtraciones.

Si bien este trabajo no analiza todos los documentos publicados por Snowden permite tener una idea general sobre

el funcionamiento de esta agencia. Se espera que sirva como fuente inicial para futuras investigaciones sobre la vigilancia masiva en Internet.

II. Recolección de información

La herramienta “Informante sin Límites” permite a la NSA saber cuánta información se ha recolectado y desde donde se lo ha hecho. A través de un mapa interactivo se puede ver la cantidad de llamadas telefónicas y comunicaciones de internet interceptadas[1].

En el libro “Sin un Lugar Donde Esconderse” Glenn Greenwald detalla[2] que en 30 días la NSA había recolectado “*97 mil millones de e-mails y 124 mil millones de llamadas telefónicas de todo el mundo.*” Además este programa permite ver cuántas comunicaciones se interceptan por país.

¿Cómo hace la NSA para recolectar tanta información a nivel global? Según una diapositiva[3] secreta de la NSA existen cinco formas en que esta agencia lo puede hacer como muestra la figura 1.

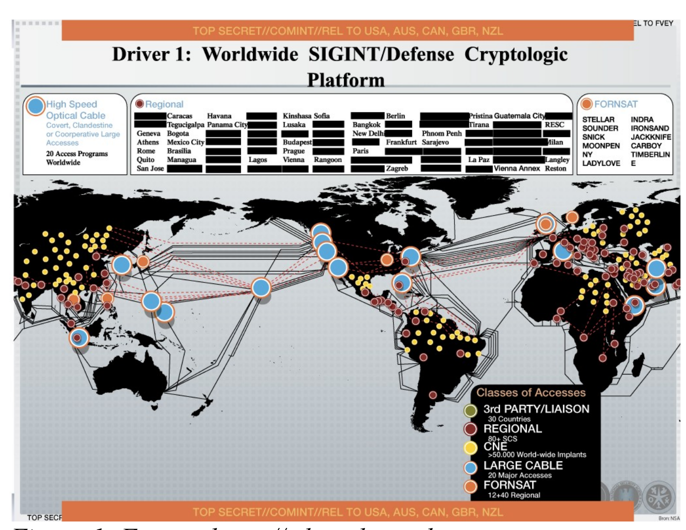


Figura 1: Fuente: https://edwardsnowden.com

El portal Electrospaces.net realizó un análisis basado en este y otros documentos[4]. El mismo determinó que: 3rd PARTY/LIASON se refiere a la información recolectada en colaboración con otras agencias, REGIONAL a la información que obtiene a través de embajadas y consulados en el mundo, CNE a la que se obtiene mediante ataques informáticos, LARGE CABLE a la información que se accede a través de empresas de comunicaciones y FORNSAT a través de la interceptación comunicación de satélites.

A. *Colaboración con otros Países*

Según Greenwald existen tres niveles de relación entre la NSA y agencias de otros países[2]. En primer lugar se encuentran la Alianza de los Cinco Ojos de la que son miembros Gran Bretaña, Canadá, Nueva Zelanda y Australia. La NSA colabora con estos países para espiar y no los espía salvo que funcionarios de dichos países lo soliciten. En segundo lugar se encuentran países con los que la NSA establece alianzas específicas pero que a su vez son espiados agresivamente. En tercer lugar se encuentran el resto de países con los que la NSA no comparte información y que siempre son espiados. En la figura 2 se puede ver un documento[5] de 2013 que muestra los 2 primeros niveles de cooperación y organismos multilaterales con los que también podrían compartir información.



Figura 2: Fuete: https://edwardsnowden.com

Gran parte de los documentos del archivo de Snowden que están clasificados como secreto máximo son compartidos con las agencias de inteligencia de los países de la Alianza de los Cinco Ojos.

La GCHQ es la agencia de vigilancia de Reino Unido y la colaboradora más estrecha de la NSA. Esta agencia mantiene el programa de recolección de datos llamado TEMPORA. Un documento secreto de la GCHQ dice que TEMPORA puede almacenar datos y metadatos para que estos luego sean accedidos por sistemas como XKEYSCORE. Según el documento “TEMPORA almacena 10 veces más información que el segundo XKEYSCORE más grande”.[6]

La información se recolecta principalmente a través de los cables de Internet que atraviesan Reino Unido para conectar Europa con Estados Unidos. Esto se logra gracias a la colaboración de empresas como Vodafone,Verizon y BT[7].

B. *Embajadas y Consulados*

En octubre de 2013 el semanario Alemán Der Spiegel publicó un artículo donde explica la forma en la que la NSA pudo haber espiado a Angela Merkel[8]. La investigación revela la existencia de unidades conformadas por agentes de la NSA y la CIA conocida como “Servicio Especial de Recolección” (*SCS* por sus siglas en inglés) que operan en embajadas y consulados alrededor del mundo.

En diciembre de 2013 el diario Italiano L'Espresso[9] realizó otra investigación basada en los documentos de Snowden donde se muestra que en Italia SCS trabaja en las ciudades de Roma y Milán. En las dos investigaciones se destaca el hecho de que los agentes que trabajan en embajadas y consulados disponen de inmunidad diplomática.

Según L'Espresso en 2002 existían alrededor de 65 oficinas SCS en el mundo y para 2010 este número creció a 80. En la figura número 1 se puede ver un listado parcial de las mismas dentro del cuadro *Regional*.

Las dos investigaciones denuncian la existencia de antenas de interceptación de comunicaciones celulares ubicadas en los edificios de las embajadas norteamericanas. Las antenas se ocultan detrás de ventanas falsas cubiertas con paneles dialéctricos que no interfieren con la transmisión de ondas radioeléctricas. A través de las mismas podrían interceptar las comunicaciones de celulares en las ciudades del mundo donde operan.

C. En Colaboración con Empresas de Comunicaciones e Internet

La NSA emplea directamente a unas 30,000 personas y además mantiene contratos con 60,000 que trabajan en empresas privadas. Tal es el caso de Snowden que trabajó dentro de las oficinas de la NSA, pero oficialmente era empleado de empresas como Dell y Booz Allen Hamilton[2].

El nombre de las empresas que colaboran es un secreto resguardado por la agencia. En la figura 3 se puede ver una diapositiva[10] que muestra el nombre de algunas de ellas y las áreas en las que operan.



Figura 3: Fuente: https://edwardsnowden.com

La unidad de Operaciones de Fuentes Especiales (SSO por sus siglas en inglés) es la encargada de manejar las relaciones entre la NSA y las corporaciones tecnológicas.

Gran parte de la recolección de datos se las hace directamente a través de los principales cables de fibra óptica que son operados por empresas norteamericanas. Esto se lo realiza a través de programas que llevan nombres como BLARNEY, FAIRVIEW y STORMBREW.

En el año 2015 The New York times realizó una investigación[11] donde comparó información de los documentos de Snowden con noticias conocidas. A través de esto logró determinar que el programa FAIRVIEW se refiere a AT&T, mientras que STORMBREW se refiere al trabajo realizado con Verizon.

La NSA aprovecha el poder estratégico de las redes de fibra óptica operadas por empresas norteamericanas para interceptar comunicaciones y analizarlas luego en sistemas como XKEYSCORE[12]. El análisis de The New York Times da a entender que el trabajo entre la NSA y las empresas de comunicaciones se realiza en los mejores términos. Pero si esto no fuera así, la NSA puede recurrir a presiones legales como la que hizo a Verizon para recolectar metadatos de las comunicaciones de millones de usuarios dentro de Estados Unidos en 2013[13].

BLARNEY es un programa paraguas que abarca a otros programas. El más conocido es PRISM donde participan empresas de Internet como Microsoft, Google, Yahoo, Facebook, Youtube, Skype y Apple. Estas empresas dan acceso a la información como correos electrónicos, chats, videos, fotos, llamadas de voz/ip, archivos, actividad en redes sociales y más[14] como se puede ver en la figura 4.

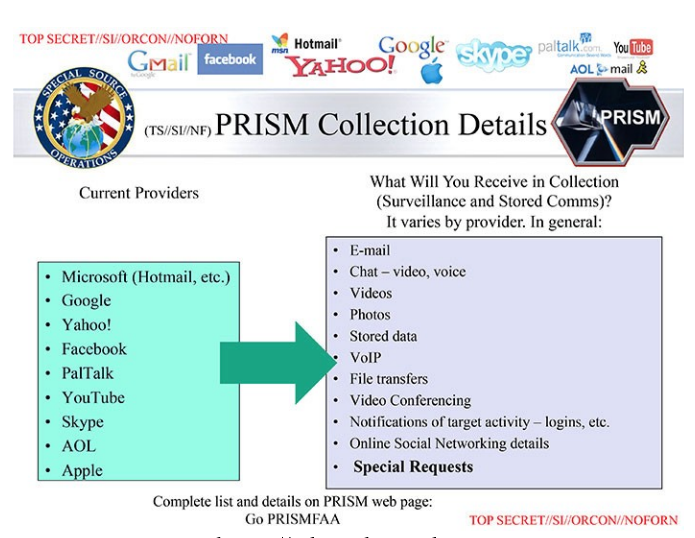


Figura 4: Fuente: https://edwardsnowden.com

A diferencia de STORMBREW y FAIRVIEW la información no se la entrega de forma masiva a la NSA. Esta se almacena en los servidores de las empresas y agentes de la NSA deben realizar solicitudes para acceder al contenido. Este trabajo se hace en conjunto con el FBI que es la agencia que interactua directamente con la empresas.

Para realizar una solicitud de vigilancia a un objetivo esta debe ser validada para asegurarse de no espiar a un ciudadano de Estados Unidos. En caso de espiar a un norteamericano se debe conseguir una orden judicial de la corte FISA. Si el blanco de vigilancia no tiene nacionalidad estadounidense, entonces no tiene ninguna protección legal[15].

En el caso de Microsoft existe documentación que muestra su relación con la NSA y el programa PRISM. Esta empresa trabajó con el FBI para facilitar el acceso a los archivos de SkyDrive (hoy OneDrive) y ayudó a la NSA para que pueda leer el trafico cifrado de Outlook.com. Nueve meses después de haber comprado Skype se triplicó la cantidad de video llamadas recolectadas a través de PRISM[16].

Si bien en los documentos de Snowden no mencionan puertas traseras para los sistemas Windows se podría sospechar esta posibilidad. El grupo anónimo ShadowBrokers obtuvo herramientas de ataque informático pertenecientes a la NSA. Hicieron algunas publicaciones de estas herramientas en Internet y en una de ellas subieron código fuente para atacar sistemas operativos Windows. Gracias a esto se desarrollaron los *ransomware* WannaCry y Petya[17].

¿Estas herramientas de la NSA explotaban vulnerabilidades desconocidas por Microsoft o era un trabajo similar al realizado con PRISM? Probablemente nunca se tenga la respuesta ya que el funcionamiento de Windows es secreto.

D. *A través de explotación de redes*

Cuando la NSA no tiene acceso a ciertas comunicaciones busca la forma de penetrar en las redes de comunicación para accederlas. La unidad que se encarga de este trabajo se llama TAO.

Durante la mitad de la década pasada la unidad pudo atacar a 258 objetivos de vigilancia en 89 países. Solo en el año 2010 condujo 279 operaciones a nivel global[18].

Para realizar los ataques los agentes de TAO buscan vulnerabilidades en los sistemas utilizados en las redes que quieren espiar. Der Spiegel cita un ejemplo en el cuál al utilizar el sistema XKEYSCORE se puede identificar tráfico solicitando la actualización de un sistema Windows. Esta información resulta útil para TAO porque le permite identificar las vulnerabilidades que el sistema quiere parchar. Una vez conocida la vulnerabilidad es fácil realizar el ataque[19].

Corporaciones como AT&T y Verizon tienen acceso a gran parte del tráfico de internet pero no a todo. Por este motivo a la NSA le resulta interesante poder atacar los sistemas que administran otros cables submarinos de fibra óptica. Tal es el caso del cable submarino SEA-ME-WE-4 que conecta a Europa con el norte de África, los países del Golfo Pérsico, las costas de India, Malasia y Tailandia.

Para poder recolectar información de este cable, TAO tuvo la misión de atacar a las empresas operadoras del mismo. En ese entonces eran France Telecom (hoy Orange) y Telecom Italia Sparkle[20].

Otra forma de atacar a las redes que se desea espiar consiste en enviar equipamiento de hardware con *malware* preinstalado. Para esto la NSA intercepta los paquetes de dispositivos de telecomunicaciones del correo tradicional. Una vez interceptado el paquete, se lo abre y se implanta una puerta trasera. Luego se lo devuelve para que llegue a su destino final. Un documento secreto de junio de 2010 muestra imágenes de un *switch* de marca Cisco[21]. Con esta estrategia sería fácil interceptar las comunicaciones de redes LAN en instituciones públicas.

La criptografía es una herramienta indispensable si se desea proteger las comunicaciones. Esto puede llegar a complicar el trabajo de análisis de información. Para esto la NSA tiene el departamento conocido como Servicio de Criptoanálisis y Explotación (CES por sus siglas en inglés).

Der Spiegel realizó una investigación extensa sobre los esfuerzos de la NSA para vulnerar las seguridades de las comunicaciones en internet[22]. Según la misma, en el año 2013 CES tenía un presupuesto $34.3 millones de dólares.

Entre los trabajos que realiza la NSA se encuentra el de descifrar tráfico de redes VPNs o vulnerar las conexiones HTTPS. Incluso intenta influenciar a los organismos de estandarización como IETF para debilitar los estándares de comunicaciones seguras.

Sin embargo, en el mismo reportaje se menciona herramientas que la NSA todavía no ha podido vulnerar. La investigación muestra correos cifrados con PGP y mensajes de chat cifrados con OTR que no se pudieron descifrar. En lo que se refiere al anonimato en internet Tor seguía siendo un problema para la NSA.

Cabe destacar que las herramientas que la NSA no podía vulnerar son todas software libre. Esto es una ventaja ya que el código fuente de estos sistemas puede ser auditado lo que dificulta la posibilidad de añadir puertas traseras. Además se pueden distribuir libremente por lo que se podría masificar su uso sin una barrera económica.

E. *A Través de Señales Satelitales*

En agosto de 1988 el periodista británico Donald Campbell reveló un programa de espionaje global de comunicaciones satelitales llevado a cabo por la NSA y la GCHQ conocida como ECHELON. En ese entonces ya se utilizaba computadoras para filtrar información relevante.[23]

Esta información no tuvo mayor impacto hasta que en el año 2001 el Parlamento Europeo publicó un informe sobre ECHELON donde se confirmó su existencia. El mismo se sustentó verificando la existencia de estaciones terrestres para vigilar satélites, material desclasificado, el testimonio de periodistas como Duncan Campbell y Nicky Hager, así como también de empleados de las agencias de inteligencias[24].

Según Campbell los documentos de Snowden confirman la existencia de ECHELON pero con el nombre FORNSAT.[25] La descripción de este programa consiste en estaciones terrestres alrededor del mundo que interceptan las comunicación de los satélites en el espacio. A diferencia de las antenas parabólicas que apuntan a un satélite las antenas en estas estaciones son esféricas para apuntar a varios satélites a la vez.[26]

La estación de Menwith Hill ubicada en Reino unido es la que más información recolecta pero no es la única. En la figura 5 se puede ver un mapa mundial con las estaciones de FORNSAT distribuidas alrededor del mundo[27].

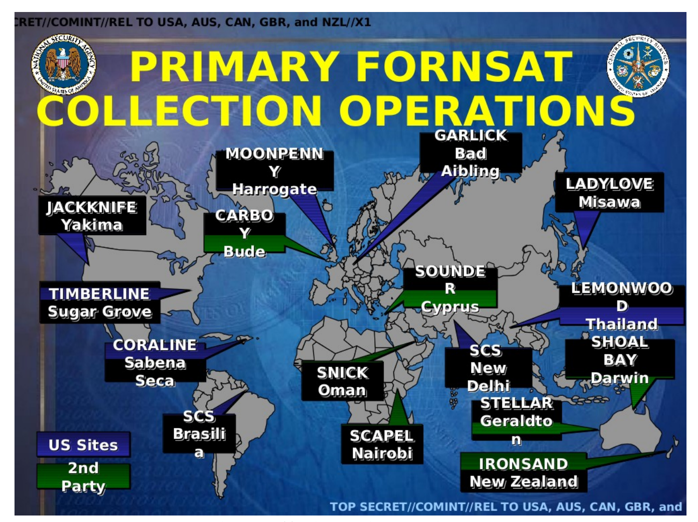


Figura 5: Fuente: https://edwardsnowden.com

III. ANÁLISIS DE INFORMACIÓN

La NSA cuenta con diversos sistemas para analizar la información recolectada. En una presentación[28] titulada “Filtrado Inteligente de tus datos: casos de estudio Brasil y México”(Traducción propia del inglés) la NSA describe cómo pudo acceder a información relevante de un mar de datos. Según ellos “Se podría encontrar una aguja en un pajar de una forma repetitiva y eficiente” (Traducción propia del inglés)

En su primera aparición pública Edward Snowden dijo: "Yo, sentado en mi escritorio, tenía la facultad de intervenir al que fuera, desde un contador hasta un juez federal e incluso el presidente, siempre y cuando tuviera su correo electrónico personal."[29]

El programa de vigilancia al que hacía referencia es XKEYSCORE que permite analizar tráfico de Internet recolectado por la NSA. Si bien XKEYSCORE es uno de los programas más documentos en el archivo de documentos de Snowden, no es el único que analiza la información recolectada. Sin embargo un análisis de sus capacidades permite imaginar los alcances de procesamiento de información de la NSA.

Para el año 2009[30] tenía la capacidad de realizar búsquedas del contenido de las comunicaciones de Internet de hasta tres días y metadatos hasta treinta días de antigüedad como se puede ver en la figura 6.

TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

“Slowing down the Internet”

KEYSCORE

- XKS goal is to store the full-take content for 3-5 days, effectively “slowing down the Internet” so that analysts can go back and recover sessions that otherwise would have been dropped by the front end
- Meta-data is saved off longer, with the goal of 30 days retention
- A lot of analysis can be done through meta-data only (MARINA is meta-data only)

TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

Figura 6: Fuente https://edwardsnowden.com

Las comunicaciones que resulten más interesantes se podrían almacenar por más tiempo en otros sistemas. Por ejemplo, el sistema PINWALE permite almacenar información hasta por cinco años[31].

En el año 2015 el medio digital The Intercept realizó una investigación titulada “XKEYSCORE: Google de la NSA para el mundo de las Comunicaciones Privadas” (Traducción propia del inglés). La misma se basa en 48 documentos filtrados por Snowden[32].

Según la investigación, la NSA podría analizar el tráfico que viaja por Internet y realizar búsquedas sobre el mismo. Gran parte del tráfico de internet viaja cómo texto plano. Esto es muy conveniente para la NSA ya que permite realizar búsquedas sobre el mismo con gran nivel de detalle.

A través de un buscador similar al de Google se podría buscar los correos electrónicos de una persona. Se podría realizar filtros sobre el tráfico de navegación desde una determinada IP o desde un *cookie* del navegador web asociado a un blanco de vigilancia.

Incluso se puede llegar a realizar búsquedas basadas en texto. Por ejemplo, se podría realizar búsquedas de todas las comunicaciones de un país donde exista algún texto determinado. De esta manera sin tener un objetivo de vigilancia determinado, al espiar las comunicaciones de todos se podrían identificar sospechosos.

Si bien la criptografía es una muy buena herramienta para ocultar el contenido de los mensajes, se suele utilizar sin ocultar los metadatos. Gracias a esto la NSA podría realizar búsquedas de todos los correos cifrados de un país y determinar a quienes vigilar más extensivamente. No porque sean sospechosos de algo, sino porque protegen sus comunicaciones.

IV. OPERACIONES REVELADAS

La NSA sostiene que estos programas se realizan con el objetivo de luchar contra el terrorismo. Varios documentos publicados muestran que esto no siempre es así.

Dentro de una presentación digital del 21 de mayo de 2009[33] se muestra un listado parcial de 10 presidentes de un total de 122 líderes a nivel mundial. En el mismo se encuentra la canciller alemana Angela Merkel, pero también los entonces presidentes de países latinoamericanos como Perú, Guatemala y Colombia.

Estos no son los únicos líderes latinoamericanos que han sido espiados por la NSA. En una presentación de 2012[28] se muestra como se espió las comunicaciónes de la entonces presidenta de Brasil Dilma Rousseff cómo se puede ver en la figura 7. La misma presentación también muestra que se espió al entonces candidato a presidente de México Enrique Peña Nieto (hoy presidente). El espionaje se realizó sobre las comunicaciones de los dos líderes y de varios de sus asesores cercanos.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 surge effort

(U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

Figura 7: Fuente: https://edwardsnowden.com

Peña Nieto no es el único presidente mexicano en ser espiado. En el año 2010 la NSA logró tomar control sobre el servidor de correo electrónico de la presidencia de México. Gracias a esto se empezó a recolectar las comunicaciones del presidente y su gabinete[34].

Espiar a líderes políticos del mundo pone a los Estados Unidos en ventaja sobre otros países. Esto se puede ver claramente cuando se trata de negociaciones internacionales. Existen documentos que muestran que los Estados Unidos, a través de la NSA, espió a las Naciones Unidas incluyendo al secretario general y el Consejo de Seguridad[2].

Al finalizar la Cumbre de las Américas de 2009 el entonces subsecretario de Estado, Thomas Shannon, escribió al jefe de la NSA: "informes recibidos por la NSA nos permitieron conocer a fondo los planes e intenciones de los otros participantes de la cumbre."[2]

El espionaje también se lo realiza para obtener información sobre los recursos estratégicos de los Estados. Tal es el caso del espionaje que realizó la NSA sobre los altos ejecutivos de PDVSA. Para la NSA "entender PDVSA es entender el corazón económico de Venezuela"[35] (Traducción propia del inglés).

El Centro Seguridad de las Comunicaciones de Canadá (CSEC por sus siglas en Inglés) espió en conjunto con la NSA al Ministerio de Minas de Brasil[36]. Tres de las cuatro empresas mineras más grandes del mundo son canadienses. Tener información interna y las comunicación del ministerio daría ventaja a empresas de Canadá al momento de negociar contratos de explotación minera.

Conocer como piensan naciones enteras resulta útil para poder influenciar la opinión pública de estos países. Esto fue lo que intentó hacer Reino Unido a través de la GCHQ para favorecer la imagen de las Islas Malvinas como territorio británico en América Latina.[37]

V. Otras Agencias de Inteligencia

En 2011 Wikileaks publicó documentos de empresas que venden herramientas de vigilancia a gobiernos alrededor del mundo. Según esta filtración la empresa VASTech, de Sudáfrica, oferta equipamiento con la capacidad para interceptar las comunicación de naciones enteras. Empresas como SS8 de Estados Unidos, HackingTeam de Italia y Vupen de Francia desarrollan troyanos para secuestrar computadoras y teléfonos celulares.[38]

Si existen empresas que venden tecnología de vigilancia para gobiernos entonces deben existir gobiernos que compran estas soluciones. En 2015 los sistemas de la empresa HackingTeam fueron vulnerados y se publicaron en Internet 400 gigabytes de archivos confidenciales, que entre otros, incluían correos electrónicos y código fuente. En la figura 8 se puede puede ver marcado con azul los países donde agencias gubernamentales contrataron servicios con HackingTeam.[39]

Esta es una de las muchas empresas que vende servicios de espionaje digital a gobiernos. Esto quiere decir que las agencias de inteligencia de todo el mundo no necesitan desarrollar tecnología propia para poder realizar espionaje digital ya que existe un mercado de empresas ofertando este servicio.

Si bien cualquier gobierno puede comprar herramientas de vigilancia, ninguno tiene la capacidad de espiar en Internet que tiene la NSA. Esto se debe a la facilidad de recolectar información, en particular por el dominio que tienen las empresas de tecnología norteamericanas como se describió en la sección 2C de este documento.

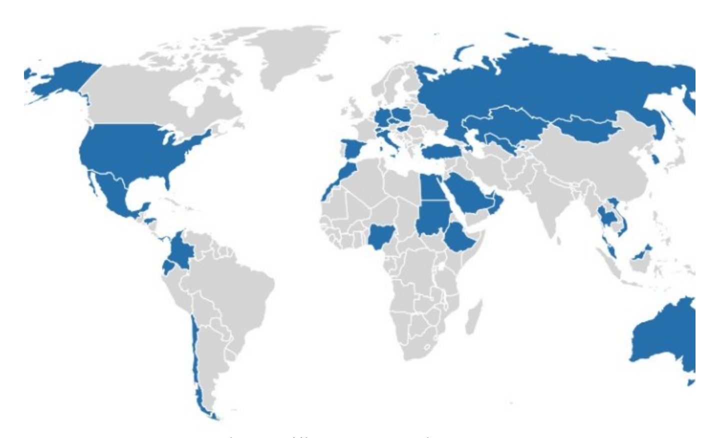


Figura 8: Fuente: https://hipertextual.com

VI. Conclusiones

La información expuesta en el presente trabajo permite entender como la NSA recolecta y analiza información, así como también, el tipo de operaciones que puede realizar con estas capacidades

Gracias al trabajo coordinado con empresas como Verizon y AT&T, o través del programa TEMPORA de la GCHQ, la NSA copia y almacena el tráfico que viaja por el *backbone* de Internet.

Las que participan en programa PRISM como Google, Microsoft, Yahoo, Apple, Facebook y otras, son fuente de información para la NSA. Si bien la agencia no tiene acceso directo a los servidores de estas empresas, lo solicita a través del FBI que interactuá directamente con ellas. Es decir son por lo menos dos las agencias pueden acceder a la información de PRISM.

Con el objetivo de interceptar comunicaciones celulares en ciudades alrededor del mundo existen las unidades SCS. Las mismas están conformadas por agentes de la CIA y la NSA que operan como funcionarios diplomáticos por lo que gozan de inmunidad. En 2010 existían ochenta de estas unidades en embajadas y consulados alrededor del mundo.

Las comunicaciones satelitales son espiadas desde estaciones terrestres distribuidas por el mundo a través del programa FORNSAT. En 1988 esto ya fue denunciado por el periodista británico Duncan Campbell cuando este programa se lo conocía como ECHELON.

Cuando la NSA no tiene acceso a cierta información recurre a los ataques informáticos para obtenerla. TAO es la unidad que realiza este trabajo. Solo en 2010 realizó 299 operaciones en todo el mundo.

Existen varios sistemas con los que la NSA puede procesar la información recolectada. XKEYSCORE es un buscador, similar al de Google, que permite realizar búsquedas sobre comunicaciones privadas. A través del mismo se podría, por ejemplo, obtener correos electrónicos, chats, comunicaciones de voz sobre IP, historial de navegación, entre otros.

Si la comunicación esta cifrada podría complicar el trabajo de la NSA. Sin embargo existe el Servicio de Criptoanálisis y Explotación que busca las formas de superar los protocolos de cifrado. Ya sea a través de medios tecnológicos u otros como influenciar a organismos de estándares.

Las capacidades que tiene la NSA son empleadas con fines que van más allá de la guerra contra el terrorismo. Se las utiliza para buscar beneficio político o económico para Estados Unidos y sus aliados. Los ejemplos sobran, pero se puede mencionar algunos. Espiar al secretario Secretario General de Naciones Unidas o presidentes de países. Conocer los recursos mineros y petroleros de Brasil y Venezuela. Utilizar la información recolectada para beneficiar la opinión pública sobre Gran Bretaña y las Malvinas en América Latina a través de campañas mediáticas.

La información expuesta en este documento ya era de conocimiento público. A pesar de esto los servicios de empresas pertenecientes a PRISM son ampliamente utilizados. En países como Ecuador o Argentina se ofertan los planes de celular con WhatsApp (propiedad de Facebook) ilimitado sin consumir datos. Los clientes no son informados sobre los riesgos a la privacidad que sufren al utilizar estos servicios.

Cada vez son más las universidades que utilizan los servicios en la nube de empresas como Google o Microsoft para facilitar la comunicación y la colaboración dentro de estas organizaciones. ¿Son conscientes los rectores y decanos que contratan estos servicios sobre los riesgos a la privacidad?

La NSA no es la única agencia que espía las comunicaciones digitales. Gobiernos alrededor del mundo contratan herramientas de vigilancia de empresas denunciadas en los Spy Files. ¿Existe transparencia sobre el uso de estas herramientas en las agencias gubernamentales? Sin los controles adecuados podrían ser utilizadas en contra de los propios ciudadanos.

Internet esta cambiando la forma en la que vive la sociedad moderna de una manera que todavía no se acaba de comprender. Nunca antes fue tan fácil investigar sobre cualquier tema, expresar ideas de forma pública o comunicarse de forma rápida y barata con cualquier persona sin importar su ubicación geográfica. De la misma manera nunca antes fue posible vigilar de forma masiva las comunicaciones de millones de personas a nivel mundial.

Es importante buscar soluciones para que la sociedad pueda aprovechar los beneficios de Internet sin poner en riesgo la privacidad de las personas. Se debe democratizar la seguridad informática para que cualquier persona pueda utilizar Internet y comunicarse de forma segura.

Descentralización de las comunicaciones, masificar del uso de criptografía mediante herramientas de software libre son posibilidades que se deben investigar. Sin embargo, lo más importa es generar conciencia en la sociedad de que existe un problema, solo entonces se podrá encontrar soluciones.

AGRADECIMIENTOS

A Edward Snowden que arriesgó su vida para que se pueda conocer la verdad sobre la vigilancia a nivel mundial.

A la Universidad de Buenos Aires por todo el conocimiento brindado en la Maestría de Seguridad Informática .

REFERENCIAS

[1] G. Greenwald y E. MacAskill, “Boundless Informant: the NSA’s secret tool to track global surveillance data”, The Guardian, 11-jun-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining. [Consultado: 19-jun-2017].

[2] Greenwald, Glenn, Snowden. Sin un Lugar Donde Esconderse, 1a ed. Colombia: Ediciones B, 2014.

[3] “Worldwide SIGINT/Defense Cryptologic Platform”. [En línea]. Disponible en: https://edwardsnowden.com/2013/11/23/worldwide-sigintdefense-cryptologic-platform/.

[4] “NSA’s global interception network”, Electrospaces.net, 03-dic-2013. [En línea]. Disponible en: https://electrospaces.blogspot.com.ar/2013/12/nsas-global-interception-network.html. [Consultado: 19-jun-2017].

[5] McCarthy, Tom, “New NSA tool to quantify, track intelligence collection revealed – live | World news | The Guardian”, 08-jun-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jun/08/nsa-surveillance-prism-obama-live. [Consultado: 18-ene-2017].

[6] “TEMPORA — “The World’s Largest XKEYSCORE” — Is Now Available to Qualified NSA Users”. [En línea]. Disponible en: https://edwardsnowden.com/2014/07/23/tempora-the-worlds-largest-xkeyscore-is-now-available-to-qualified-nsa-users/.

[7] J. Ball, L. Harding, y J. Garside, “BT and Vodafone among telecoms companies passing details to GCHQ”, The Guardian, 02-ago-2013. [En línea]. Disponible en: https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq. [Consultado: 28-jun-2017].

[8] Appelbaum, Jacob et al., “Embassy Espionage: The NSA’s Secret Spy Hub in Berlin - SPIEGEL ONLINE - International”, SPIEGEL ONLINE, 27-oct-2013. [En línea]. Disponible en: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html. [Consultado: 11-may-2017].

[9] S. Maurizi y G. Greenwald, “Revealed: How the Nsa Targets Italy”, l’Espresso, 05-dic-2013. [En línea]. Disponible en: http://espresso.repubblica.it/inchieste/2013/12/05/news/revealed-how-the-nsa-targets-italy-1.144428. [Consultado: 15-may-2017].

[10] “NSA Strategic Partnerships | Courage Snowden”. [En línea]. Disponible en: https://edwardsnowden.com/2014/05/15/nsa-strategic-partnerships/. [Consultado: 29-jun-2017].

[11] J. Angwin, C. Savage, J. Larson, H. Moltke, L. Poitras, y J. Risen, “AT&T Helped U.S. Spy on Internet on a Vast Scale”, The New York Times, 15-ago-2015. [En línea]. Disponible en: https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html. [Consultado: 22-jun-2017].

[12] “SSO Corporate Portfolio Overview”. [En línea]. Disponible en: https://edwardsnowden.com/2015/08/18/sso-corporate-portfolio-overview/. [Consultado: 30-jun-2017].

[13] G. Greenwald, “NSA collecting phone records of millions of Verizon customers daily”, The Guardian, 06-jun-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. [Consultado: 17-abr-2017].

[14] Gellman, Barton y Poitras, Laura, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program - The Washington Post”, 07-jun-2013. [En línea]. Disponible en: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. [Consultado: 16-oct-2016].

[15] "Electrospaces.net: What is known about NSA's PRISM program", Electrospaces.net, 23-abr-2014. [En línea]. Disponible en: http://electrospaces.blogspot.com.ar/2014/04/what-is-known-about-nsas-prism-program.html. [Consultado: 18-ene-2017].
[16] G. Greenwald, E. MacAskill, L. Poitras, S. Ackerman, y D. Rushe, "Microsoft handed the NSA access to encrypted messages", The Guardian, 12-jul-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data. [Consultado: 09-mar-2017].
[17] Barret, Brian, "The Encryption Debate Should End Right Now", WIRED, 30-jun-2017. [En línea]. Disponible en: https://www.wired.com/story/encryption-backdoors-shadow-brokers-vault-7-wannacry/. [Consultado: 01-jul-2017].
[18] Appelbaum, Jacob, L. Poitras, Laura, M. Rosenbanch, Stöcker, Christian, Schindler, Jörg, y Stark, Holger, "Inside TAO : Documents Reveal Top NSA Hacking Unit (part 1)", Spiegel Online, 29-dic-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html. [Consultado: 01-jul-2017].
[19] Appelbaum, Jacob, L. Poitras, M. Rosenbanch, Stöcker, Christian, Schindler, Jörg, y Stark, Holger, "Inside TAO : Documents Reveal Top NSA Hacking Unit (part 2)", Spiegel Online, 29-dic-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-2.html. [Consultado: 01-jul-2017].
[20] Appelbaum, Jacob, Poitras, Laura, M. Rosenbanch, Stöcker, Christian, Schindler, Jörg, y H. Stark, Holger, "Inside TAO : Documents Reveal Top NSA Hacking Unit (part 3)", Spiegel Online, 29-dic-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html. [Consultado: 01-jul-2017].
[21] "Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets | Courage Snowden". [En línea]. Disponible en: https://edwardsnowden.com/2014/05/14/stealthy-techniques-can-crack-some-of-sigints-hardest-targets/. [Consultado: 01-jul-2017].
[22] Appelbaum, Jacob et al., "Prying Eyes: Inside the NSA's War on Internet Security", SPIEGEL ONLINE, 28-dic-2014. [En línea]. Disponible en: http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html. [Consultado: 03-ene-2017].
[23] D. Campbell, "They've got it taped", 12-ago-1988. [En línea]. Disponible en: http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf.
[24] McCarthy Kieren, "This is how we know Echelon exists", 14-nov-2001. [En línea]. Disponible en: https://www.theregister.co.uk/2001/09/14/this_is_how_we_know/. [Consultado: 16-jul-2017].
[25] D. Campbell, "NSA: 'yes, there is an ECHELON system' | DuncanCampbell.org". [En línea]. Disponible en: http://www.duncancampbell.org/content/nsa-yes-there-echelon-system. [Consultado: 17-jul-2017].
[26] Gallagher, Ryan, "The NSA's British Base at the Heart of U.S. Targeted Killing", The Intercept, 06-sep-2016. [En línea]. Disponible en: https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/. [Consultado: 14-jul-2017].
[27] "Primary FORNSAT Collection Operations". [En línea]. Disponible en: https://edwardsnowden.com/2014/07/23/primary-fornsat-collection-operations/. [Consultado: 17-jul-2017].
[28] "Intelligently filtering your data: Brazil and Mexico case studies". [En línea]. Disponible en: https://edwardsnowden.com/2013/12/18/intelligently-filtering-your-data-brazil-and-mexico-case-studies/. [Consultado: 10-may-2017].
[29] B. M. Tecnología, "La poderosa herramienta de EE.UU. para vigilarlo todo en internet", BBC Mundo, 01-ago-2013. [En línea]. Disponible en: http://www.bbc.com/mundo/noticias/2013/08/130801_tecnologia_snowden_nsa_xkeyscore_dp. [Consultado: 22-abr-2017].
[30] "X-KEYSCORE as a SIGDEV tool". [En línea]. Disponible en: https://edwardsnowden.com/2015/07/22/x-keyscore-as-a-sigdev-tool/. [Consultado: 03-mar-2017].
[31] G. Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", The Guardian, 31-jul-2013. [En línea]. Disponible en: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. [Consultado: 02-feb-2017].
[32] M. Marquis-Boire, G. Greenwald, y L. Micah, "NSA's Google for the World's Private Communications", The Intercept, 01-jul-2015. [En línea]. Disponible en: https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/. [Consultado: 02-feb-2017].
[33] "Content Extraction Analytics", Content Extraction Analytics, 21-may-2009. [En línea]. Disponible en: https://edwardsnowden.com/2014/06/26/content-extraction-analytics/.
[34] L. Poitras, J. Glüsing, M. Rosenbanch, y H. Stark, "NSA Accessed Mexican President's Email", SPIEGEL ONLINE, 20-oct-2013. [En línea]. Disponible en: http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html. [Consultado: 11-may-2017].
[35] Greenwald, Glenn y Fishman, Andrew, "Overwhelmed NSA Surprised to Discover Its Own Surveillance 'Goldmine' on Venezuela's Oil Executives", The Intercept, 18-nov-2015. [En línea]. Disponible en: https://theintercept.com/2015/11/18/overwhelmed-nsa-surprised-to-discover-its-own-surveillance-goldmine-on-venezuelas-oil-executives/. [Consultado: 26-may-2017].
[36] "American and Canadian Spies target Brazilian Energy and Mining Ministry", Fantástico, 06-oct-2013. [En línea]. Disponible en: http://g1.globo.com/fantastico/noticia/2013/10/american-and-canadian-spies-target-brazilian-energy-and-mining-ministry.html. [Consultado: 26-may-2017].
[37] Fishman, Andrew y G. Greenwald, "Britain Used Spy Team to Shape Latin American Public Opinion on Falklands", 02-abr-2015. [En línea]. Disponible en: https://theintercept.com/2015/04/02/gchq-argentina-falklands/. [Consultado: 01-jul-2017].
[38] "WikiLeaks - The Spy Files", 01-dic-2011. [En línea]. Disponible en: https://wikileaks.org/the-spyfiles.html. [Consultado: 06-sep-2017].
[39] F. Palazuelos, "Los países iberoamericanos que usaron a Hacking Team", Hipertextual, 06-jul-2015. [En línea]. Disponible en: https://hipertextual.com/2015/07/los-paises-iberoamericanos-que-usaron-a-hacking-team-para-espiar. [Consultado: 28-ago-2017].

Rafael Bonifaz es ingeniero en sistemas de la Universidad San Francisco de Quito. Lleva más de 10 años promoviendo la adopción del software libre y 5 sensibilizando sobre la importancia de la privacidad en el mundo digital y los riesgos de la vigilancia en Internet. Actualmente se encuentra cursando la Maestría de Seguridad Informática en la Universidad de Buenos Aires. Para su proyecto de especialización investiga los documentos revelados por Snowden.